Annual Progress Report
Grant No. NAG1-1123

DEVELOPMENT OF A SOFTWARE SAFETY PROCESS AND A CASE STUDY OF ITS USE

Submitted to:

Dr. Dave E. Eckhardt, M/S 478
National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681-0001

Submitted by:

John C. Knight
Professor

Report No. UVA/528344/CS96/102
September 1995

DEPARTMENT OF COMPUTER SCIENCE

SCHOOL OF
ENGINEERING
& APPLIED SCIENCE

University of Virginia
Thornton Hall
Charlottesville, VA 22903

Annual Progress Report
Grant No. NAG1-1123

DEVELOPMENT OF A SOFTWARE SAFETY PROCESS AND A CASE STUDY OF ITS USE

Submitted to:

Dr. Dave E. Eckhardt, M/S 478
National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681-0001

Submitted by:

John C. Knight
Professor

Department of Computer Science
SCHOOL OF ENGINEERING AND APPLIED SCIENCE
UNIVERSITY OF VIRGINIA
CHARLOTTESVILLE, VIRGINIA

Report No. UVA/528344/CS96/102
September 1995

Copy No._____

TABLE OF CONTENTS

OVERVIEW

The goal of this research is to continue the development of a comprehensive approach to software safety and to evaluate the approach with two case studies. The case studies are a major part of the project, and they involves the analysis of specific safety-critical systems—one from the medical equipment domain and one from the nuclear power domain. The particular applications being used were selected because of the availability of suitable candidate systems. We consider the results to be generally applicable and in no way particularly limited by the domains.

With more and more important functions in existing and proposed safety-critical systems being implemented by computers, concern over the role of software in such systems has increased. An especially important area is that class of systems for which safety rather than reliability or availability is the overriding issue. Some research that addresses the safety of software specifically has been reported but many open questions remain. In particular, no complete process is available for engineers to follow when building applications software for systems in which safety considerations dominate. We are developing such a process through a combination of theoretical and empirical research.

The research is concentrating on issues raised by the specification and verification phases of the software lifecycle. The theoretical research is based on our framework of definitions for software safety in which the problem is broken down into *specification safety* and *implementation safety.*

In the area of specification, the main topics being investigated are:

- the development of a comprehensive technique for specification capture,
- the formal specification of complex user interfaces,
- the reuse of specifications through the development of certified libraries of reusable specification components, and
- the development of rigorous techniques for the preparation of software safety specifications.

A second area of theoretical investigation is the development of verification methods tailored to the characteristics of safety requirements. Verification of the correct implementation of the safety specification is central to the goal of establishing safe software. In the area of specification, the main topics being investigated are:

- the application of *specification limitation* to permit certain classes of safety problems to be eliminated by exhaustive testing in reasonable amounts of time, and
- the development of a complete test set for certain properties by automatic derivation from the safety specifications for specifications written in a suitably formal notation such as `Z'.

The empirical component of this research is focusing on two case studies in order to provide detailed characterizations of the issues as they appear in practice, and to provide a testbed for the evaluation of various existing and new theoretical results, tools and techniques. The systems being used in the case studies are the *Magnetic Stereotaxis System* (MSS), a safety-critical medical system presently under development and the *University of Virginia's research nuclear reactor* (UVAR). The overall, long term approach being taken in the empirical research using these systems is to develop fully functional software of sufficient quality to be suitable for safety-critical use. This approach is necessary to ensure that the research undertaken is not weakened by unrealistic assumptions or restrictions. The empirical research is implementing the various techniques resulting from the theoretical research and using these implementations to assess the theoretical results.

Research results to date are documented in various papers and reports, and they are not repeated here. Copies of these papers and reports have been supplied to the sponsor under separate cover.

The remainder of this report is organized as follows. In the next section, details of students funded under this grant are documented. Seminars presented describing work under this grant are listed in the following section, and the final section lists publications resulting from this grant.

SUPPORTED STUDENTS

During the reporting period, the following students were supported in whole or in part under this grant:

Name	-	Kevin G. Wika
Dissertation Title	-	Safety Kernel Enforcement of Software Safety Policies
Degree	-	Ph.D.
Status	-	Graduated 5/95.
Name	-	Ambar sarkar
Dissertation Title	-	Integrating Operational Specification with Performance Modeling for Digital-System Design.
Degree	-	Ph.D.
Status	-	Graduated 5/95.
Name	-	Darrel M. Kienzle
Degree	-	Ph.D.
Status	-	changed research fields.
Name	-	R. Gregory Wohlford
Degree	-	MCS.
Status	-	Graduated 5/95.
Name	-	Shannon B. Wrege
Degree	-	BS.
Status	-	Graduated 5/95.
Name	-	Ricardo D. Chiappe
Degree	-	BS.
Status	-	In progress.
Name	-	Charles R. Odell
Degree	-	BS.
Status	-	In progress.
Name	-	Michael Lee
Degree	-	BS.
Status	-	In progress.

SEMINARS

In addition to papers presented at conferences that are listed in the next section, seminars describing the research being performed under this grant were presented at the following institutions during the reporting period:

- Georgia Institute of Technology, Atlanta, GA.
- Clemson University, Clemson, SC.

PUBLICATIONS

During the reporting period, the following papers resulting in part from work under this grant either appeared in print, were presented at professional meetings, or were accepted for publication:

1. Knight, J.C. and K.G. Wika, "Software Safety in a Medical Application", *Journal of Image Guided Surgery*, to appear.

2. Elder, M.C. and J.C. Knight, "Specification of User Interfaces for Safety-Critical Systems", *MRCAS '95, Second International Symposium on Medical Robotics and Computer Assisted Surgery*, November 1995, Baltimore, MD.

3. Knight J.C. "Limitations of Mathematics in Software Engineering", *MDS '95, Conference on the Mathematics of Dependable Systems*, Institute of Mathematics and its Applications, September 1995, York, England.

4. Wika, K.G. and J.C. Knight, "On the Enforcement of Software Safety Policies", *10th Annual IEEE Conference on Computer Assurance (COMPASS '95)*, June 1995, Gaithersburg, MD.

5. Knight, J.C., "Safety Analysis", *Third Annual NASA Langley Formal Methods Workshop*, May 1995, Hampton, VA.

6. Knight, J.C. and K.G. WIka, "Generalized Implementation of Software Safety Policies", *Nineteenth Annual Goddard Software Engineering Workshop*, November, 1994, Greenbelt, MD.

7. Dunn, M.F. and J.C. Knight, "The Role of Domain Analysis in Quality Assurance", *Twelfth Pacific Northwest Software Quality Conference*, September 1994, Portland OR.

During the reporting period, the following papers resulting in part from work under this grant were prepared as technical reports. Many have been or will be submitted for publication in the near future:

1. Knight, J.C., L.G. Nakano, and A. Sarkar, "Eliciting Background Information for Safety-critical Software Specification", TR-95-42 (September 1995) Department of Computer Science, University of Virginia, Charlottesville, VA 22903 (submitted to ICSE 18).

2. Knight, J.C., K.G. Wika, and S.D. Wrege, "Exhaustive Testing as a Verification Technique", TR-95-41 (September 1995) Department of Computer Science, University of Virginia, Charlottesville, VA 22903.

3. Knight, J.C., and A.G. Cass, "Achieving Software Quality Through Reuse", TR-95-40 (September 1995) Department of Computer Science, University of Virginia, Charlottesville, VA 22903.

4. Sullivan K.J., and J.C. Knight, "Assessment of an Architectural Approach to Large-Scale Systematic Reuse", TR-95-37 (August 1995) Department of Computer Science, University of Virginia, Charlottesville, VA 22903 (submitted to ICSE 18).

5. Elder, M.E., "Specification of User Interfaces for Safety-Critical Systems", TR-95-30 (July 1995) Department of Computer Science, University of Virginia, Charlottesville, VA 22903.

6. Wika, K.G., "Safety Kernel Enforcement of Software Safety Policies", TR-95-24 (May 1995) Department of Computer Science, University of Virginia, Charlottesville, VA 22903.

DISTRIBUTION LIST

1 - 3	Dr. Dave E. Eckhardt, M/S 478 National Aeronautics and Space Administration Langley Research Center Hampton, VA 23681-0001 (804) 864-1698
4	Mr. Joseph S. Murray Grants Officer, M/S 126 Acquisition Division National Aeronautics and Space Administration Langley Research Center Hampton, VA 23681-0001 (804) 864-7709
5 - 6**	National Aeronautics and Space Administration Scientific and Technical Information Facility P.O. Box 8757 Baltimore/Washington International Airport Baltimore, MD 21240
7	J. C. Knight
8	J. M. Ortega
*	Postaward Research Administration
9 - 10	Marcy Rodeffer, Clark Hall
11	SEAS Preaward Administration Files

* Cover Letter Only

** 1 bound and 1 unbound copy.

JO#6612:pa